UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,677	11/14/2003	Amir Peles	RADW 20.114	2877

26304 7590 04/10/2007
KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
POWERS, WILLIAM S	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,677	PELES, AMIR	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

No Information Disclosure Statement was submitted.

Claim Objections

1. Claims 23, 26, 28, 30 and 31 are objected to because of the following informalities:

a. As to claim 23, the claim depends from claim 25. For purposes of examination, the Examiner assumes that the claim depends from claim 18.

b. As to claims 26, 28 and 30, each of the claims recites the limitation "said network device" in line 2 of each claim. There is insufficient antecedent basis for this limitation.

c. As to claim 31, the claim is missing the preposition "to" in line 4. In addition, the claim recites the limitation, "said authentication request messages" in line 7. There is insufficient antecedent basis for this limitation.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 6, 15, 16, 26 and 31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claim 6, 16 and 26, the term "transparent" as used in the claim language contradicts the meaning of the term from the Microsoft Computer Dictionary. In the claim, transparent is explained as not modifying the IP address or the contents of an authentication message. According to the Microsoft Computer Dictionary, transparent is the quality of a "device, function, or part of a program that works so smoothly and easily that it is invisible to the user." To one of ordinary skill in the art, transparent does not mean that an authentication message IP address and data is not modified. It means that the message is delivered regardless of the route that the message has to take through the communications network.

As to claim 16, the verb "may" in line 9 to further limit the system. May is not a definitive word and, as such, introduces uncertainty at to whether or not said user request-issuing device is included in a network access server or in a user network.

As to claim 31, it is not clear from the claim language how many user request-issuing devices are claimed in the limitations or how many connections there are between the entities of the claim. Is there one user request-issuing device with three

different connection configurations or are three user request-issuing devices, each with different connection requirements? In addition, the limitation "a user request-issuing device operatively connected to a service policy director" (lines 15-16) is repeated in lines 17-18.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 7,073,055 to Freed et al. (hereinafter Freed).

As to claim 1, Freed teaches:

a. Receiving authentication messages for a user at said network device (Freed, column 14, lines 8-30).

b. Determining user identifiers and service attributes associated with said user (Freed, column 14, lines 8-30).

c. Creating a user service policy entry in a user policy table for said identified user containing said service attributes (Freed, column 18, lines 10-27).

d. Consulting said user policy table to determine how to manage said user traffic subsequent to said user authentication messages (Freed, column 18, lines 28-42).

e. Managing subsequent user traffic based on said consulting step (Freed, column 18, lines 28-42).

As to claim 2, Freed teaches monitoring and parsing said user authentication messages to obtain said user identity and attributes associated with said user (Freed, column 13, lines 23-26).

As to claim 3, Freed teaches said user policy table is located within said network device (Freed, column 19, lines 13-21).

As to claims 4, 10 and 14, Freed teaches said network device offers internal network services comprising at least bandwidth management (Freed, column 7, lines 53-57).

As to claims 5, 9 and 13, Freed teaches said authentication messages are using the RADIUS protocol (Freed, column 13, lines 18-48).

As to claims 6, 11 and 15, Freed teaches said network device functions in proxy mode (Freed, column 13, lines 18-47).

As to claim 7, Freed teaches:

a. Identifying a user originating said network user traffic (Freed, column 14, lines 8-30).

b. Consulting a user policy table to locate a user service policy corresponding to said user (Freed, column 18, lines 28-42).

c. Managing said network user traffic based on said consulting step by denying transmission of user traffic on the basis of access privileges and service level parameters (Freed, column 14, lines 18-56).

As to claim 8, Freed teaches said user policy table is filled according to information in user authentication messages (Freed, column 18, lines 10-27).

As to claim 12, Freed teaches:

a. Receiving authentication messages for a user at said network device (Freed, column 14, lines 8-30).

b. Determining user identifiers and service attributes associated with said user (Freed, column 14, lines 8-30).

c. Creating a user service policy entry in a user policy table for said identified user containing said service attributes (Freed, column 18, lines 10-27).

d. Consulting said user policy table to determine how to manage said user traffic subsequent to said user authentication messages (Freed, column 18, lines 28-42).

e. Managing said network user traffic based on said consulting step by denying transmission of user traffic on the basis of access privileges and service level parameters (Freed, column 14, lines 18-56).

As to claim 16, Freed teaches:

a. A user request-issuing device (CPE) (Freed, column 6, lines 45-54 and figure 1).

b. A service provider network over which user authentication messages and user traffic originated by said user request-issuing device is transmitted (ISP) (Freed, column 14, lines 8-17 and figure 5).

c. An authentication server to which said user request-issuing device attempts to connect and by which said user request-issuing device is authenticated and registered (RADIUS) (Freed, column 13, lines 18-48 and figure 5).

d. A service policy director independent of said authentication server, enforcing a service policy for said user request-issuing device (Freed, column 7, lines 46-52).

e. Said user request-issuing device may be included in a user network (Freed, column 6, lines 45-54 and figure 5).

As to claim 17, said service policy director includes a user policy table (user profile in network service provider entity) (Freed, column 18, lines 10-27).

As to claim 18, Freed teaches said user policy table includes user identifier information and service attribute information (Freed, column 18, lines 10-27).

As to claim 19, Freed teaches said user identifier includes at least an Internet/intranet address (Freed, column 17, line 64-column 18, line 9).

As to claim 20, Freed teaches said user identification information further includes at least the username (Freed, column 16, lines 45-54).

As to claim 21, Freed teaches wherein said attribute information includes any one or more of the following: access privileges parameters, traffic logging mechanisms and user activity statistics entitlement parameters, security services entitlement parameters, or service quality level parameters (Freed, column 18, lines 10-42).

As to claim 22, Freed teaches said service quality level parameters include any one or more of the following: a bandwidth limit, a bandwidth guarantee or a bandwidth priority (Freed, column 19, lines 1-3).

As to claim 23, Freed teaches said service attributes define services offered by said service policy director, said services including any one or more of the following: classification of network user traffic, modification of network user traffic, forwarding of network user traffic, or logging of single network user traffic statistics (Freed, column 17, lines 40-50).

As to claim 24, Freed teaches said network device offers internal network services including one of bandwidth management, access control or network usage statistics (Freed, column 8, lines 5-18).

As to claim 25, Freed teaches a plurality of said service policy directors reside on a network (Freed, column 7, lines 46-52).

As to claim 26 as best understood, Freed teaches said network device including said service policy director functioning in a transparent mode, wherein authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages (the network device does not modify the IP address or data of either the Access-Accept or Access-Reject messages) (Freed, column 13, line 4-column 14, line 56).

As to claim 27 as best understood, Freed teaches said service policy director functioning in said transparent mode receives said user authentication request

messages addressed to said authentication server and forwards said user authentication request messages to said authentication server (Freed, column 13, line 4-column 14, line 56).

As to claim 28, Freed teaches said network device including said service policy director functioning in a proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses on said authentication messages without any modification to the data of said authentication messages (Freed, column 13, lines 18-47).

As to claim 29, Freed teaches said service policy director functioning in said proxy mode receives said user authentication request messages addressed to said service policy director and forwards it to said authentication server (Freed, column 13, line 4-column 14, line 56).

As to claim 30, Freed teaches said service policy director functioning in a passive mode, wherein the authentication messages in a provider network are copied to the network device (Freed, column 18, lines 10-42).

As to claim 31 as best understood, Freed teaches:

a. A user request-issuing device operatively connected to a service policy director, said service policy director connected to an authentication server and

said authentication server being operatively connected to said user request-issuing device, wherein said service policy director receives said user authentication request messages addressed to said authentication server and forwards said user authentication request messages to said authentication server (Freed, column 13, line 4-column 14, line 56).

b. A user request-issuing device operatively connected to a service policy director, said service policy director connected to an authentication server and said authentication server being operatively connected to said user request-issuing device, wherein said service policy director receives said user authentication request messages addressed to said authentication server and forwards said user authentication request messages and queries said authentication server (Freed, column 13, line 4-column 14, line 56).

c. A user request-issuing device operatively connected to a service policy director, said service policy director receiving copied network user traffic, said copied network user traffic copied by a network device, and said user-request issuing device being operatively connected to said service policy director, the service policy director receives a copy of said user authentication request messages addressed to and destined for said authentication server (Freed, column 13, line 4-column 14, line 56).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

4/4/2007

William S. Powers
Examiner
Art Unit 2134

KAMBIZ ZAND
PRIMARY EXAMINER